

一种动态分级密钥管理方案的设计与分析

于 江, 苏锦海, 戴紫彬

(信息工程大学 电子技术学院, 河南 郑州 450004)

摘 要: 在分析了分级访问控制中密钥管理方案所存在问题的基础上, 针对动态的分级结构, 使用对称密码设计了支持动态结构的分级密钥管理方案, 方案的密钥生成和推导过程运算开销小. 方案使用了临时参数的设计, 较好地支持了安全组的加入和退出, 密钥更新的效率较高, 参数的存储空间占用较小.

关键词: 分级访问控制; 分级密钥管理; 密钥推导

中图分类号: TP309.2

文献标识码: A

文章编号: 1000-7180(2011)05-0071-04

Design and Analysis for a Dynamic Hierarchical Key Management Scheme

YU Jiang, SU Jin-hai, DAI Zi-bin

(Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: Cryptographic techniques for hierarchical access control have attracted intensive research interests recently. There are many differences of the key management schemes in hierarchical access control scenarios. This paper proposes a new key management scheme which can be used for access control in dynamic hierarchies. The scheme can generate and derive hierarchical keys with high performance and can support the security classes insert and delete in dynamic. The key renewal can be performed with little system spending and the public parameters for each class is small.

Key words: Hierarchical Access Control (HAC); Hierarchical key management; key derivation

1 引言

计算机网络的快速发展, 信息和数据的激增, 为广大用户提供了极大的可访问资源, 但如何有效地共享信息和访问信息, 对访问控制技术的研究提出了更高的要求. 分级的访问控制是针对多级安全模型设计的访问控制机制, 解决多级安全中用户访问权限与信息资源的等级对应问题. 分级系统中, 用户可以按安全权限分成不相交的用户组集合: $S = \{SC_1, SC_2, \dots, SC_n\}$, 在集合上定义一个二元偏序关系“ $\leq$ ”, 如果 $SC_i \leq SC_j$ 就表示用户组 SC_i 的安全级别不高于用户组 SC_j 的安全级, SC_j 对 SC_i 的信息具有访问权限, 从而 $(S, \leq)$ 构成一个偏序集 (partially ordered set, poset). 从密钥掌握的角度来看, SC_j 中的用户可以得到 SC_i 的密钥, 而 SC_i 中

的用户则不能得到 SC_j 的密钥.

Akl 和 Taylor 首次将密钥和等级系统的访问控制问题相结合, 基于 RSA 问题设计分级密钥方案, 虽然方案较简单, 但实现比较困难. Mackinnon 等人对 Akl-Taylor 方案进行了改进, 但需要占用大量存储空间, Lin-Hwang-Chang 方案^[1]减少了公开关系参数的数量. 目前提出的分级访问控制的密钥管理研究方案中, 有的使用公钥密码和多项式问题实现分级密钥的管理, 有的使用对称密码或 hash 函数进行分级密钥的推导. 使用公钥密码的分级方案中用户可直接推导出其后代安全组的密钥, 但用户需要存储的密钥参数较多, 密钥推导运算量大, 对动态的分级结构支持不好, 密钥更新时系统开销较大. 文中针对动态的分级访问控制结构, 设计了使用对称密码的分级密钥管理方案.

2 相关研究方案分析

目前流行的访问控制方式是基于角色的访问控制,通过分配和取消角色来完成用户权限的授予和取消,或以可信度为基础的角色管理^[2],针对网格系统还基于信任度的访问控制^[3].以密码为基础的访问控制方式主要针对密钥的分配和管理进行研究,在分级访问控制密钥管理方案中,使用对称密码和单向 hash 函数的方案一般具有运算量小,用户需要存储的安全参数少,密钥更新时对分级结构影响相对较少等优点,但是上级对所属下级的密钥的推导无法直接进行,需要逐级的链式运算.

Zhong 方案^[4]和 Yang-Li 方案^[5]使用 hash 函数实现密钥的分级方案,密钥的推导只需要简单的 hash 运算.

使用对称密码算法的分级密钥方案如 Sandhu^[6]和 Lin^[7]方案,使用分组密码算法实现分级密钥间关系参数的生成和推导,方案的密钥推导效率较高,用户存储的关系参数较少.但由于方案中关系参数的生成过程中分级密钥直接参与运算,所以存在着与 Zhong 方案同样的安全组退出后密钥和关系参数更新的问题.

文献^[8]中的方案考虑了动态的分级结构中密钥管理问题,安全组的加入和密钥更新时只需要操作与当前安全组直接相关的密钥,但安全组删除时则会影响到其所有后代的密钥和参数.

3 动态的分级密钥管理方案

针对目前分级密钥的动态性管理问题,文中使用对称密码设计分级密钥管理方案,方案中包括:分级密钥的生成、密钥的推导、安全组加入和退出的密钥更新.

3.1 方案定义

分级结构的偏序集 $(SC, \leq)$ 的结构可以由非循环有向图表示,记为 $G = (V, E)$, v 表示所有的组(或称为节点、顶点等)的集合,在分级访问控制中表示安全组; E 表示安全组之间的有向边偏序关系的集合.在分级结构的上定义的密钥管理方案包括密钥生成算法 GEN 和密钥推导算法 DER,他们的定义如下:

(1) 密钥生成算法 GEN 使用对称密码算法,输入参数为:随机数空间 ρ ,有向图 G ;输出结果为:用户安全组的秘密参数 S 和密钥 K ,公开的关系参数 R .记为 $GEN(\rho, G)$.

(2) 密钥推导算法 DER 的输入参数为:有向图 G ,有偏序关系的两个安全组 SC_i 和 SC_j ,且 $SC_i \leq SC_j$, SC_j 的秘密参数 S_j ,公开参数 R ;输出参数为: SC_i 的密钥 K_i .记为 $DER(G, SC_i, SC_j, S_j, R)$.

在方案中需要使用三种密码算法:

(1) 安全参数生成算法 $H, H: \{0, 1\}^e \times \{0, 1\}^* \rightarrow \{0, 1\}^e$,即输入 ρ 的密钥和的数据能输出 ρ 的伪随机序列;

(2) 加密算法 E ,输入密钥和明文能输出密文;

(3) 解密算法 D ,输入解密密钥和密文能输出明文.

安全参数生成算法 H 可以使用对称分组加密算法直接构造得到带密钥的杂凑函数,可与加密算法 E 使用同一对称算法,减少方案中的算法数量.权威中心负责生成和管理关系参数.

3.2 密钥生成算法

分级结构中安全组的密钥生成算法 $GEN(\rho, G)$ 过程描述如下:

(1) 对于任意一个安全组 $SC_i \in V$,选择随机数 $S_i \in \{0, 1\}^e$ 和 $K_i \in \{0, 1\}^e$, S_i 作为 SC_i 的秘密参数, K_i 作为 SC_i 的秘密密钥,由权威分配给用户;

(2) 使用 SC_i 的标识 SID 计算 $t_i = H_{S_i}(SID_i \oplus K_i)$ 作为生成关系参数的临时参数;

(3) 对于任意两个安全组 $SC_i, SC_j \in V$ 如果存在偏序关系 $(SC_i, SC_j) \in E$,计算 $p_{ij} = H_{t_i}(SID_j)$ 和 $R_{ij} = E_{p_{ij}}(t_j \parallel K_j)$;

(4) 公开 R_{ij} 为 SC_j 和 SC_i 的关系参数;

(5) 重复步骤(1)~(4),使安全类 SC_i 遍历分级结构中所有的安全组.

密钥生成算法 $GEN(\rho, G)$ 中存在从偏序关系到公开参数和秘密参数两个映射关系:

$$Pub: (SC_i, SC_j) \rightarrow R_{ij}$$

$$Sec: SC_i \rightarrow (S_i, K_i)$$

3.3 密钥推导算法

对于具有分级关系的 $SC_i, SC_j \in V$ 如果存在偏序关系 $(SC_i, SC_j) \in E$,那么 SC_i 推导其所属下级 SC_j 的密钥过程如下:

(1) 取出自己的秘密参数 S_i 和身份标识 SID_i 计算 $t_i = H_{S_i}(SID_i \oplus K_i)$;

(2) 设 $(\omega_0, \omega_1), \dots, (\omega_{m-1}, \omega_m)$,这里 $\omega_0 = SC_i, \omega_m = SC_j$,是一条从 SC_i 到 SC_j 的最短的路,执行以下计算:

$$t_u = t_i;$$

$$\text{for } (u = 0; u < m; u++)$$

```

{
  获得关系参数  $R_{u,u+1}$  和  $SID_{u+1}$ ;
   $p_{u,u+1} = H_{t_u}(SID_{u+1})$ ;
   $t_{u+1} \parallel K_{u+1} = D_{p_{u,u+1}}(R_{u,u+1})$ ;
   $t_u = t_{u+1}$ ;
   $k = K_{u+1}$ ;
}
Return  $k$ ;
 $SC_i$  最终获得  $SC_j$  的密钥  $K_j$  即  $k$ .

```

3.4 分级密钥的动态管理

方案中密钥的动态管理主要针对两个安全组之间偏序关系的增加和删除,安全组的加入和删除这两组操作。

(1) 增加偏序关系

设 (SC_u, SC_v) 是一个要增加的偏序关系,则计算 $p_{uv} = H_{t_u}(SID_v)$ 和 $R_{uv} = E_{p_{uv}}(t_u \parallel K_v)$,将关系参数 R_{uv} 公开。

(2) 删除偏序关系

设 $(SC_u, SC_v) \in E$ 是已存在的偏序关系,如果要删除该偏序关系,需要做到删除关系后防止 SC_u 中的用户继续推导出 SC_v 和其下属的安全组的密钥。定义 $SC_m \in A_v, A_v$ 表示集合 $\{SC_w : SC_w \leq SC_v, SC_w \in V\}$,即所有与 SC_v 有偏序关系的后代。

删除操作首先为 SC_m 选择新的秘密密钥 $K'_m \in \{0,1\}^p$ 并计算 $t'_m = H_{S_m}(SID_m \oplus K'_m)$,对于其他的每一个与 SC_m 有关的偏序关系 $(SC_l, SC_m) \in E$ 计算 $p'_{lm} = H_{t'_l}(SID_m)$ 和 $R'_{lm} = E_{p'_{lm}}(t'_l \parallel K_m)$,将新的关系参数 R'_{lm} 公开。删除偏序关系时,并不需要改变 SC_m 的秘密参数 S_m 。删除操作达到的结果是将 SC_v 及其所有的后代的密钥和关系参数全部更新。

(3) 加入安全组

一个新的安全组 SC_u 加入到分组结构中时,进行两步操作完成他的加入。首先,为该安全组分配身份标识 SID_u ,选择秘密参数 $S_u \in \{0,1\}^p$ 和秘密密钥 $K_u \in \{0,1\}^p$,计算临时参数 $t_u = H_{S_u}(SID_u \oplus K_u)$;然后使用增加偏序关系的算法为 SC_u 增加上下级的偏序关系。

(4) 删除安全组

从分级结构中删除一个安全组 SC_u 时,同样需要两步操作。首先,使用删除偏序关系的算法删除所有进入和流出 SC_u 的偏序关系;然后,权威中心将与 SC_u 相关的秘密参数和关系参数删除。

(5) 密钥更新

当一个安全组 SC_u 需要更新其当前使用的密钥

时,需要以下步骤完成:选择新的秘密密钥 $K'_u \in \{0,1\}^p$,计算新的临时参数 $t'_u = H_{S_u}(SID_u \oplus K'_u)$,更新秘密映射 $\text{Sec} : SC_u \rightarrow (S_u, K'_u)$;所有与 SC_u 有偏序关系的直接上级和直接下级都需要重新计算与 SC_u 之间的关系参数。

密钥更新过程中只需要更新 SC_u 的秘密参数和密钥,其他安全组不需要改变秘密映射和参数,只需要改变关系参数。

4 安全性分析

方案的安全性依赖于所选择的对称密码算法,在密钥空间足够大的前提下,对称算法需要满足在攻击者对密钥的破译时在计算上不可行。下面从几种对分级密钥的主要攻击方式入手分析方案的安全性。

4.1 反向攻击

攻击者希望利用低安全级别的密钥计算得到高安全级别用户的密钥。如果 A 希望破解其父亲的密钥,他首先获得一个包含其父亲密钥的关系参数,假设为 $R_{ij} = E_{p_{ij}}(t_j \parallel K_j)$, K_j 为其父亲的密钥, A 要获得 K_j 需要解决的困难是破译对称算法的密钥,在计算上是不可行的。

如果 A 有 m 个父组,他希望通过这 m 个关系参数结合计算得到秘密信息,需要破解的是 $R_{(i+m)j} = E_p(t_j \parallel K_j)$, $m = 1, \dots, m$,由于每一个关系参数加密运算时使用的密钥 p 都不相同,所以难度同于破解对称算法。

4.2 共谋攻击

某一个安全组 SC_i 有两子组分别是 SC_j, SC_k ,如果 SC_j, SC_k 希望利用他们掌握的秘密参数和密钥协作攻击得到他们父安全组的密钥 K_i ,由于关系参数生成时 SC_i 的秘密密钥并未直接参数运算,而是经过两次 H 函数的运算后作为密钥参与关系参数的计算,所以, SC_j, SC_k 无法直接利用 R_{ij}, R_{ik} 获取有用信息,还需要破解两次 H 函数,难度比反向攻击还大。

4.3 同胞攻击

安全组 SC_i, SC_j 有共同的父亲组 SC_k ,如果 SC_i 试图获得同胞 SC_j 的密钥,他要么获得父亲组的临时参数,要么直接破解关系参数 R_{kj} ,获得父亲组的临时参数需要破解对称算法和 H 函数,破解关系参数的难度是只知道密文的情况下破译密钥,难度比反向攻击都大。

4.4 外部攻击

外部攻击是指一个在分级结构之外的攻击者,希望通过收集关系参数来获得用户的密钥 K_i . 很明显,攻击者需要进行的是唯密文攻击对称算法,是不可行的.

5 性能和效率分析

通过与 Lin-Hwang-Chang、Zhong、Lin 方案的比较,考查了方案在密钥生成和密钥推导过程中的计算量,以及用户存储参数和密钥的数量. 设分组结构中有 n 个安全组, L 表示偏序关系的数量, D 表示从一个组到其后代组的平均距离,表 1 列举了本方案与其他几种方案复杂度的对比.

表 1 本方案与其他方案的复杂度对比

	密钥生成	密钥推导	秘密参数的数量	公开参数的数量
Lin-Hwang-Chang	$O(n^2)$	$O(n\log n)$	$O(n)$	$O(n^2\log n)$
Zhong	$O(L)$	$O(D)$	$O(n)$	$O(n^2)$
Lin	$O(L)$	$O(D)$	$O(n)$	$O(n^2)$
本方案	$O(n)$	$O(D)$	$O(n)$	$O(n^2)$

从表中可以看出本方案的计算时间复杂度与使用对称密码和 Hash 函数的方案都是 $O(n)$,比使用非对称密码的方案时间复杂度小,而且公开参数的存储空间占用也比使用非对称密码的方案小. 文中案主要针对分级结构的动态性设计,方案中增加了一个临时参数,使安全参数不必直接参与关系参数的计算,密钥更新时只需要更新与该组相关的安全组的关系参数,而不必更新整个结构中的密钥,安全组的退出和加入对分组结构影响较小.

6 结束语

在分级结构中使用密码技术实现用户组的分级访问控制是一种有效的访问控制机制,分级密钥方案的设计需要考虑效率、安全性、动态性等因素. 文中使用对称密码算法设计了安全可行的分级密钥管

理方案,密钥的生成和推导过程运算开销小、密钥更新的效率较高. 同时充分考虑的对分级结构动态性的变化,安全组的加入和退出只影响变发生变化的安全组本身.

参考文献:

[1] Lin I C, Hwang M S, Chang C C. A new key assignment scheme for enforcing complicated access control policies in hierarchy[J]. Future Generation Computer Systems, 2003,19(4):457—462.

[2] 顾韵华, 李丹, 陈玮. 基于谁可信度的角色访问控制模型[J]. 微电子学与计算机, 2009,26(7):5—8.

[3] 张志强, 卢昱, 孙远运. 信息网格中基于信任的访问控制研究[J]. 微电子学与计算机, 2009, 25(11):199—201.

[4] Zhong S. A practical key management scheme for access control in a user hierarchy[J]. Computers and Security, 2002, 21(8):750—759.

[5] Yang C, Li C. Access control in a hierarchy using one-way functions, elsevier [J]. Computers and Security, 2004(23):659—664.

[6] Sandhu R S. Cryptographic implementation of a tree hierarchy for access control[J]. Information Processing Letter, 1988, 27(2):95—98.

[7] Lin C H, Lee W, Ho Y K. An efficient hierarchical key management scheme using symmetric encryptions[C]// Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05). Washington, DC, USA:IEEE Computer Society, 2005:399—402.

[8] Lin C H. Hierarchical key assignment without public-key cryptography[J]. Computers and Security, 2001, 20(7):612—619.

作者简介:

于江 男,(1978—),博士研究生. 研究方向为网络安全.

苏锦海 男,(1963—),博士,教授. 研究方向为网络安全、密钥工程.

戴紫彬 男,(1966—),教授. 研究方向为信息安全、密码微系统设计.